REMARKS

Applicants appreciate the thorough examination of the present application that is evidenced in the Official Action of April 19, 2006 (the "Official Action"). Applicants respectfully request reconsideration of the rejections set forth therein for the reasons provided below.

1. The Independent Claims are Patentable Over Arrow and Anand

Independent Claims 1 and 33-35 stand rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 6,175,917 to Arrow et al. ("Arrow") in view of U.S. Patent No. 6,370,599 to Anand at al. ("Anand"). Applicants respectfully submit that Arrow and Anand fail to teach Independent Claims 1 and 33-35, either alone or in combination.

Independent Claim 1 recites as follows (emphasis added):

> 1. A method of performing security processing in a computing network comprising a local unit having an operating system kernel executing at least one application program, comprising:
>
> receiving a first request at the operating system kernel from the application program to initiate a communication with a remote unit;
>
> **providing a second request from the operating system kernel to a security offload component which performs security handshake processing, the second request directing the security offload component to secure the communication with the remote unit**; and
>
> providing a control function in the operating system kernel for initiating operation of the security handshake processing by the security offload component.

Similarly, Independent Claim 33 recites (emphasis added):

> 33. A method of performing security processing in a computing network including a local unit having an operating system kernel executing at least one application program, comprising:
>
> providing a security offload component which performs security session establishment and control processing;
>
> providing a control function in the operating system kernel for initiating operation of the security session establishment and control processing by the security offload component;
>
> **receiving a request at the operating system kernel from the application program to initiate a communication with a remote unit**; and
>
> **directing the security offload component to secure the communication with the remote unit in response to the request**.

Independent Claims 34-35 are system and computer program product claims containing recitations similar to those of Independent Claim 33. Applicants respectfully submit that at least the highlighted recitations of Claims 1 and 33, and the corresponding recitations of Claims 34-35, are not disclosed by Arrow and Anand, either alone or in combination.

The Official Action cites Arrow as teaching the above highlighted recitations from Claims 1 and 33, and the corresponding recitations of Claims 34-35. (Official Action at 2-4). Arrow discloses a virtual private network (VPN) in which VPN units perform security management functions for clients over a shared network. (See, e.g., Arrow, col. 5, l. 51 to col. 6, l. 23; and Arrow, col. 6, l. 62 to col. 7, l. 12). In this network, all data must be routed through the VPN units. (Arrow, col. 6, ll. 57-59; and Arrow, fig. 1). Once a VPN unit receives an inbound or outbound data packet, the VPN unit checks a lookup table or similar memory mechanism to determine whether the source and/or destination addresses of the packet are members of a VPN. (Arrow, col. 7, ll. 26-33; and Arrow, col. 8, ll. 24-29). The data communication will only be secured, if necessary, when both the source and destination addresses of the data packet belong to the same VPN. (Arrow, fig. 2, element 220; and Arrow, col. 7, ll. 46-50). VPN units maintain and edit the lookup tables based on configuration requests or commands sent by the VPN management station. (Arrow, col. 12, ll. 22-33; and Arrow, fig. 1, element 160). Therefore, the VPN unit decides when to secure the communication between a local and remote client based on information from the VPN management station.

In sharp contrast to the system described in Arrow, Claim 1 recites "providing a **second request from the operating system kernel** to a security offload component which performs security handshake processing, the second request **directing the security offload component to secure the communication** with the remote unit." Thus in a system according to Claim 1, security processing is **not** directed by a remote VPN management station, but rather is initiated in response to a first request at the operating system kernel from the application program to initiate a communication with a remote unit, which is followed by a second request from the operating system kernel to a security offload component directing the security offload component to secure the communication with the remote unit.

Furthermore, Arrow specifically states that the security processing is **transparent** to the end users. (Arrow, col. 7, ll. 5-7). The October 10, 2005, Official Action notes that VPN units may be implemented as software that "operates in conjunction with the communication software for connecting a remote client with its associated Internet Service Provider." (Oct. 10, 2005 Official Action at 14). Applicants respectfully submit, however, that the communication software of the local unit simply provides a means for transferring data packets across a public network, whether the packets are secure or not. Nothing in Arrow teaches or suggests that the communication software helps the VPN unit decide when to apply security processing. Moreover, there is nothing in Arrow to suggest that the communication software is even aware of which packets have been secured. Therefore, the security processing is transparent to the end user, even when the VPN unit is implemented in software. Accordingly, Applicants respectfully submit that Arrow does not anticipate Claim 1 for this additional reason.

In fact, Arrow actually teaches away from the operating system of the local unit directing the offload component to secure the communication with the remote unit. The system described in Arrow relies on maintaining identical lookup tables in each VPN unit so that the security rules for each client are consistent throughout the network. (Arrow, col. 8, ll. 29-32). This allows the VPN unit to determine when to secure communications between two clients and which compression, encryption, and authentication rules to use. (Arrow, col. 7, l. 65 to col. 8, l. 3). If the operating system of the local unit directed the offload component to secure the communication as recited in Claim 1, the VPN unit could be directed to perform security processing on data packets in a manner inconsistent with the rules stored in the lookup table. Hence, a remote unit not belonging to the same VPN as the local unit may receive an unexpectedly secured packet and vice versa. Moreover, the remote unit could receive the data in an unexpected format, thus preventing accurate processing of the packet.

For at least the reasons stated above, Applicants respectfully submit that Arrow does not teach or suggest at least the highlighted recitations of Claim 1. Anand does not provide, and the Office Action does not contend that it provides, the missing recitations to cure the deficiencies of Arrow. Therefore, the combination of the cited references fails to teach the recitations of Claim 1. However, even if Anand did provide the missing recitations, there would be no motivation to combine the two references. Arrow is directed to a system for securing communications in a manner that is transparent to the end users. Anand, on the other hand, discloses a method for selectively offloading processing tasks to save resources and improve efficiency on a computer system. Therefore, applying Anand to Arrow would eliminate the transparency to the local system that Arrow teaches. The Official Action states that there is motivation to apply Anand to Arrow because it would allow an application to "*selectively* offload tasks on a *dynamic, as-needed basis*." (Official Action at 3) (emphasis added). To the contrary, the VPN units described in Arrow must perform **all** of the security processing to ensure consistency across the enterprise-wide VPN. Thus instead of suggesting the combination relied upon in the Official Action, Anand teaches away from the combination with Arrow to produce the invention as recited in Claim 1.

Accordingly, Applicants respectfully submit that Arrow and Anand do not anticipate Claim 1, and respectfully request that the rejection of Claim 1 be withdrawn.

Similarly, Arrow and Anand do not teach receiving a request at the operating system kernel from the application program to initiate a communication with a remote unit, and directing the security offload component to secure the communication with the remote unit in response to the request, as recited in Claim 33. As noted above with respect to Claim 1, the VPN units of Arrow operate to secure communications based on information in lookup tables that are maintained according to configuration information and commands provided by the VPN management station, and not in response to a request received at the operating system kernel. Accordingly, Applicants respectfully request that the rejection of Claim 33 be withdrawn.

Independent Claims 34-35 contain recitations similar to the underlined portions of Claim 33. Consequently, Applicants submit that Claims 34-35 are patentable for the reasons explained above for Claim 33.

The Dependent Claims are Patentable Over the Cited Art

Applicants submit that dependent Claims 2-12, 14, 16-18, 20, 22-32 and 36-39 are patentable at least as being dependent upon patentable base claims. Moreover, Applicants submit that many of the dependent claims are independently patentable. For example, with respect to claim 38, the cited portion of Arrow describes an offload component retrieving configuration information for a newly authenticated client from a database at an unspecified location. (Official Action at 6). In contrast, Applicants note that Claim 38 recites the operating system kernel passing control information to the security offload component separately from the data packet. Thus, Applicants submit that Arrow does not teach or suggest the limitations of dependent claim 38.

Further, Applicants submit that with respect to Claim 39, the cited portion of Arrow describes accessing lookup tables maintained by the VPN units to determine security protocol information. In contrast, Claim 39 recites "[i]nserting security protocol information in the reserved space" of the data packet before transmitting the data packet to the remote unit. Nothing in Arrow discloses or teaches including security protocol information in the actual data packet. Thus, Applicants submit that Claim 39 is separately patentable for at least this additional reason.

Claims 36 and 37 recite reserving space in the data packet for security information prior to sending the packet to the security offload component. The cited portion of Arrow discusses standard Internet Protocol encapsulation of the data packet prior to sending the packet to a VPN unit. Nothing in Arrow discloses or teaches reserving a space in the data packet for security information prior to passing the packet to the security offload component. Moreover, the system of Arrow does not disclose or suggest passing security information within the data packets, but rather passes security information from the VPN management station directly to the security offload components. Accordingly, Applicants submit that Arrow does not teach or suggest the limitations of dependent Claims 36 and 37 for at least these additional reasons.

CONCLUSION

In light of the above remarks, Applicants respectfully submit that the above-entitled application is in condition for allowance. Favorable reconsideration of this application is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,

David C. Hall
Registration No. 38,904

Customer Number 46589
Myers Bigel Sibley & Sajovec, P.A.
P.O. Box 37428
Raleigh, NC 27627
919-854-1400
919-854-1401 (Fax)